



Bite-Size Bitcoin

A pain-free guide to
the world's largest cryptocurrency

BY LAUREL MURPHY, JON LEA &

THE COINCUB TEAM



VISIT...

LANZAROTE
Caliente.COM

Coincub

Bite-Size Bitcoin

**A pain-free guide to the world's
largest cryptocurrency**

*By Laurel Murphy, Jon Lea and the Coincub
Team*

Coincub | August 2021

© Coincub 2021 - Vetted crypto services in your country

All rights reserved - IPOI Reg No. 265792
Marine House, Clanwilliam Place, Dublin 2, Ireland

What the hell is Bitcoin, how does it work, and why won't people stop talking about it? Those are all great questions which we'll answer (mostly) in this book. Bite Size Bitcoin is your handy guide to the world's best-known cryptocurrency. We'll cover the basics and the good bits. By the time you've finished this book, you'll know how to set up a Bitcoin wallet, put bitcoins in said wallet, and keep them there. Along the way you'll learn about million dollar pizzas, heists, how the Allies won the Second World War with math, and why you should never, *ever* reuse

passwords. It'll be fun!

Table of Contents

Part 1 - Why Bitcoin?

1.1. What is Bitcoin?

1.2 Bitcoin: The Good, The Bad, and the Ugly

Part 2: How to Get Started with Bitcoin

2.1 Getting Started with Bitcoin

2.2 Exchange Reviews

2.3 How do Bitcoin Wallets Work?

2.4 An Abridged History of Exchange Hacks

Part 3: Blockchains 101

3.1 What in the Name of God is a Blockchain

3.2 Blockchain Pros and Cons

Part 4: Bitcoin in the Real World

4.1 Actually Buying Stuff with Bitcoin

4.2 Bitcoin Around the World: A Regulatory Approach

Australia
Belgium
Canada
France
Germany
Hong Kong
Hungary
India
Ireland
Japan

Part 5: Glossary

Introduction

At Coincub, we value honest, straightforward communication. In this book, you can expect a no-nonsense approach to Bitcoin. By the end of it, we hope that you'll feel empowered to make informed decisions about Bitcoin, whether that's choosing to invest or deciding to steer clear.

We're less focused on the ideology and hype behind Bitcoin and more on the practical realities, like regulation from country to country and password management. We'll also talk about some of the cool stuff too.

This book is not complete or authoritative, and does not offer any financial advice, but we hope it's helpful to you as you learn more about Bitcoin.

Part 1: Why Bitcoin?

1.1 What is Bitcoin?

Bitcoin 101

In this section, we'll give you a very quick and dirty overview of Bitcoin, introducing the important concepts so that you have a solid grounding in the basics before getting into the nitty-gritty. Throughout this book, we'll discuss the concepts covered here in more detail.

Bitcoin is a digital currency that runs on the *Bitcoin protocol*. A *protocol* is a set of rules and algorithms that govern a system. The Bitcoin protocol implementation most commonly used is called Bitcoin Core. It is open source, which means that anyone can inspect and use the code.^[1] The main point of Bitcoin is that it is *decentralized* and *censorship-resistant*. The Bitcoin protocol

has no single point of control, and it would be very difficult for any actor or state to shut down the system.

Bitcoin works because it solves the *double-spend problem* for digital currency, i.e., no one can spend the same bitcoin twice. This works because every bitcoin is unique, and every Bitcoin transaction is recorded on the Bitcoin blockchain. Blockchains are a type of distributed open ledger. In the Bitcoin blockchain, it's possible to see every transaction ever made. This way, independent *nodes* can make sure that transactions are valid. New transactions are grouped together into a *block*, which is then connected, or 'chained', to the previous block. All blocks in the Bitcoin blockchain are connected sequentially, all the way back to the first block, or the *genesis block*.

The Bitcoin blockchain functions similarly to a database, and that database is updated by *nodes* and *miners*. Up-to-date copies of the

blockchain are hosted by computers running the Bitcoin software, called *nodes*. *Miners* are computers that compete to solve extremely difficult and tedious math problems. The miner that solves the problem first wins the right to choose the next block. They are rewarded with a fixed amount of newly-minted bitcoin, as well as transaction fees associated with every transaction in the block.

A Brief History of Bitcoin

At the time of writing, it's been a little over a decade since Bitcoin was introduced. From its humble origins as a paper on a niche cryptography mailing list, Bitcoin has grown to become the progenitor of a multi-billion dollar industry, creating controversy all along the way.

To understand Bitcoin's position today, it's helpful to get a brief overview of where it's been. The story has heists, hackers, cases of

mistaken identity, and a shadowy coder at the heart of it all. Whatever the history of Bitcoin is, it's rarely boring.

To set the scene for the invention of Bitcoin, we need to go back to 2008. The worst financial crisis since the Great Depression has just gutted the global economy. Trust in central banks is at an all time low. In an effort to prevent complete financial ruin, central banks begin to utilize, among other strategies, quantitative easing.

Quantitative easing (QE) is a monetary policy used by central banks in order to stimulate the economy. By buying longer-term securities, the domestic money supply is effectively increased. Detractors referred to this as “printing money”, a not entirely accurate assessment. They argued that QE can result in the devaluation of domestic currency and inflation without economic growth.

At the same time, a cryptographer and programmer known as Satoshi Nakamoto was working on a new type of digital currency that would eliminate the need for third parties and cut out banks entirely. The website bitcoin.org was registered on August 18, 2008 via an anonymizing domain broker.^[2]

The Bitcoin whitepaper was published on a cypherpunk mailing list called metzdowd.org. Your average cypherpunk was technologically literate, interested in mathematics and politics, and had a passion for privacy and free speech. Cryptography, the mathematical and computational discipline of creating and breaking codes (more on that later) figured large in their ideology. They believed that the wide use of encryption in online communication was the best way to protect free speech and combat centralized control of the internet.^[3]

The cypherpunks were interested in making a form of digital currency that could not be

controlled or surveilled by the state or centralized banks. Prior to Bitcoin, several attempts were made to create a viable form of private digital money, like David Chaum's DigiCash, Mojo Nation for file sharing, and Adam Back's anti-email spam service HashCash. Satoshi acknowledged intellectual debts to Wei Dai's b-money, and Nick Szabo's BitGold, both of which used *proof of work* and *public key cryptography*.

Bitcoin was able to solve several of the problems associated with earlier currencies, and became a hit because of it. The Bitcoin whitepaper was published late 2008, and the first bitcoins were mined around January 3rd, 2009. The first ever transaction in the genesis block, called the 'coinbase' transaction, contained the following text:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”^[4]

The quote functions both as proof that the

first block was created in January 2009, and a rather disapproving comment on the fractional reserve banking system. The Bitcoin protocol caps the total number of coins in existence at 21,000,000. Quantitative easing is not a strategy that can be applied to Bitcoin.

The first widely documented bitcoin transaction involving physical goods happened on May 22nd, 2010, when a Florida man paid a forum user 10,000 BTC to buy him two pizzas. May 22nd is now a holiday for Bitcoiners known as Bitcoin Pizza Day. A few months later, Satoshi Nakamoto disappeared without a trace. Over 10 years later, no one has heard from Bitcoin's founder, although there are plenty of theories about who they might be.

The rise of Bitcoin was accompanied by the formation of an ideology. Bitcoiners advocated for decentralization, self-sovereignty, and a true free market. The

organisations that adopted Bitcoin at first tended to be located at the forefront or the margins of society. Silk Road, a darknet market launched in 2011, conducted all trades using Bitcoin. After several major payment platforms ended support, WikiLeaks started accepting donations in BTC.

In 2012, the Bitcoin Foundation was established to promote the development and uptake of Bitcoin.

By 2013, Bitcoin had become established enough to attract the attention of the American regulators tasked with enforcing laws against financial crime and money laundering.^[5] The first Bitcoin ATM opened in Vancouver,^[6] and the People's Republic of China started the first of many crackdowns on Bitcoin usage, barring financial institutions from using bitcoins in December. Bitcoin also hit \$1,000 USD for the first time.^[7]

2014 saw widespread acceptance of Bitcoin

as an asset class, as the U.S. Commodity Futures Trading Commission approved Bitcoin based derivative products.^[8] Disaster struck when papers leaked showing that Bitcoin exchange Mt. Gox was insolvent due to the theft of 744,408 bitcoins over a span of years. At the time, Mt. Gox was responsible for the majority of the world's bitcoin transactions. The price of Bitcoin dropped by 36% in the months following the disclosure. The fiasco went on to become legend in Bitcoin communities.

2015 and 2016 saw Bitcoin continuing to gain widespread acceptance. The Mt. Gox hack did little to dissuade people from adopting Bitcoin. In 2015, an estimated 160,000 merchants were using bitcoin, and in 2016 the number of bitcoin ATMs jumped to 700+. A major hurdle was cleared when the Cabinet of Japan recognized virtual currencies as having a function similar to real money.^[9]

The ICO (initial coin offering) craze hit in 2017, bringing with it an influx of capital and a wave of scams. A speculative bubble emerged around Ethereum-based cryptocurrency projects, where founders crowdsourced enormous amounts of money by selling tokens to investors. The tokens generally had some proposed use, and investors hoped that a token bought for pennies would skyrocket in price, just as Bitcoin had.

While many founders were committed to their projects, plenty engaged in unethical behavior. One common strategy was the “pump and dump”, where founders and advocates would talk a token up until its price rose, and then dump their holdings, making off with a fortune while the price of the token crashed.

As interest in altcoins increased, the price of Bitcoin skyrocketed, reaching just under \$19,800 in December.^{[\[10\]](#)} Bitcoin prices

plummeted in 2018 following a total ban on bitcoin trading in China. As the dust settled on the ICO bubble, countries moved to prevent financial crimes and further market manipulation by regulating cryptocurrencies. A staggering number of ICO projects failed, with nearly half of ICOs launched in 2017 going under by February 2018.[\[11\]](#)

2018 was a rough year for the crypto economy. Plenty of people had been burned. Bitcoin's price plummeted, going below \$4,000 at one point. Payment provider Stripe removed support for Bitcoin due to problems with transaction times.

Things started looking up in 2019. The Lightning network was installed, improving the speed of Bitcoin transactions. Facebook attempted to launch its own cryptocurrency, Libra. The attempt failed due to regulatory pressure, but it did signal a renewed interest in cryptocurrencies by established corporate bodies.

Just three years after the ICO craze, the price of Bitcoin skyrocketed again. Due to a price collapse where Bitcoin halved in value, combined with anxieties about the Covid-19 pandemic, buyers rushed to purchase Bitcoin. [\[12\]](#) Several large investors bought millions in Bitcoin, and payment processor PayPal announced Bitcoin functionality for US users. [\[13\]](#) The price of Bitcoin skyrocketed, and by April, 2021 the price hit \$63,000. While the price dropped down to \$30,000 in relatively short order, Bitcoin reached a historic milestone when the Legislative Assembly of El Salvador voted to make Bitcoin legal tender.

Is Bitcoin Just For Drugs and Crime?

No.

Sometimes it seems like the press about Bitcoin falls into two camps: breathless hype people convinced the Bitcoin will change the

world, and cynical naysayers that insist cryptocurrency is a giant bubble. There's good and bad aspects to Bitcoin, but it doesn't deserve much of the bad reputation it gets.

At this point in time, you can buy pretty much anything with bitcoin. Coffee, cars, computers, an apartment, illicit drugs, purebred dogs. You name it, you can buy it with bitcoin. Contrary to popular belief, bitcoin doesn't play a big role in financing crime. In 2020, the share of all cryptocurrency activity taken by criminal activity fell to 0.5%.[\[14\]](#)

How Does Bitcoin Work?

This is the section that will make you a hit in the workplace. Maybe less so at parties.

Bitcoin can seem intimidatingly complicated at first. Once you get down to it, however, it's definitely possible to get a comfortable grasp

on the underlying concepts and mechanics. This explanation doesn't cover everything, but it will hopefully give you the tools to learn more about the bits you find interesting.

First, some distinctions. Bitcoin is a peer-to-peer technology. All actions, from sending and receiving transactions to mining bitcoins are carried out collectively by a network. There's no central bank or authority.

Bitcoin was designed to solve the double-spending problem plaguing digital currency. This is not really a problem with cash. If I have \$5 and use it to buy a beer, I can't then take the same \$5 and use it to buy a shot of something interesting. However, with digital currency, it's theoretically possible to spend the same money twice. Before Bitcoin, this was generally solved by involving a central issuing body, like a bank or mint who would make and issue unique tokens.

Bitcoin solved the double spend problem in a

decentralized manner by creating a distributed ledger, the blockchain, that anyone can see and check. The Bitcoin blockchain contains a complete transaction history. People can set up computers that hold copies of the ledger, called nodes. There are two types of nodes to be aware of: *full nodes* and *light nodes*. Full nodes contain a copy of the entire Bitcoin blockchain, and are constantly updated to reflect the mining of new blocks. Light nodes, on the other hand, usually only download enough blockchain data to verify new transactions. Every time a computer is connected to the Bitcoin network in order to send or receive a transaction, it is acting as a light node.

Every new Bitcoin transaction is broadcast to the nodes. Bitcoin is a proof-of-work based protocol, which means that miners must expend electricity in the form of computational power in order to participate in bitcoin mining. They compete to solve a complex computational problem embedded in

the previous block. The first miner to solve the problem gets to choose the next block. They then broadcast the potential new block to the network. If the block is verified and added to the blockchain, the miner is rewarded with newly minted bitcoins and all the transaction fees in the block.

How do people prove that they own bitcoins? The Bitcoin protocol relies on something called public-key cryptography, which we'll get into later. For now, the important thing you know is that Bitcoin users need a public key and a private key to send bitcoins. A public key acts as a sort of address, similar to a bank account number. People can send money to public keys, and see what transactions public keys have been involved in.

A private key is needed to send any kind of transaction. You may have heard the phrase "not your keys, not your coins." This refers to the private key. If anyone has access to it,

they have full power over your bitcoins. It's vital to make sure that your private key is kept secret.

Buying a beer with Bitcoin

Let's say it's Friday night. Alice is off work, and she'd like to buy a beer. She heads off to a bar that accepts Bitcoin. She orders her beer, gets out her smartphone with her Bitcoin wallet and copies the bar's wallet address. She puts in the amount the beer costs, chooses her fee, and sends the transaction. On the surface, what happens next is a bit of waiting while the transaction goes through. But what's happening under the hood?

Alice's wallet signs the transaction with her private key. That transaction is then sent to network nodes. Full nodes hold a complete copy of the Bitcoin blockchain, which acts as a ledger. If she goes to a bar and buys a beer with Bitcoin, she's broadcasting a transaction

that is propagated through the network via something called a gossip protocol. With a gossip protocol, information spreads like a particularly juicy piece of information through an office. A few nodes get the information, who send it to a few other nodes, and so on until all nodes in the network know about the pending transaction.

Since the nodes hold full copies of the Bitcoin blockchain, they have access to the history of every transaction ever sent. With this, they can make sure that Alice hasn't already spent the bitcoins she's trying to pay with. If they verify the transaction, it gets sent to the miners.

Miners compete with each other to solve a complex math problem. The first one to succeed is rewarded with bitcoins and transaction fees. The winning miner combines pending transactions, including Alice's transaction, into a block. The block is sent out to the network back to the nodes,

who confirm that the block is valid. If everything looks correct, the nodes add the block to the previous block in the blockchain.

The bartender gets a confirmation, and Alice is free to go drink her beer until it's time for the next round.

Bitcoin transaction fees

Every time a Bitcoin transaction is made, miners need to expend computing power to mine it into a block. How are miners incentivized to confirm bitcoin transactions? The network offers a built-in reward called a miner fee.

Miners are eligible to win all the transaction fees in a block, as well as the block reward at the time. Good services will dynamically calculate miner fees. Some wallets support custom fees, and some do not.

You find out how high bitcoin transaction

fees are through wallet apps, or by searching online. Some wallet apps will dynamically inform users based on network conditions. The Bitcoin network operates with two major constraints: the average block creation time in 10 minutes, and the block size limit of 1 megabyte. The Lightning Network protocol has enabled faster transaction speeds.

Bitcoin miner fees operate on the principle of supply and demand - if there is a high amount of traffic on the network, miners will require correspondingly high fees. If you pay a very high fee, you can get the speed equivalent of priority airmail for your transaction. The size of transaction also affects the miner fee, in the same way postage varies based on the size and weight of a package.

Miners decide which transaction to confirm first based on the miner fee. If you want your transaction to be confirmed quickly, it's best to provide an appropriate miner fee.

Transaction speed

Bitcoin transactions are comparatively slow. For reference, Visa averages approximately 1,700 transactions per second (tps), while bitcoin averages 4.6 tps.^[15] Bitcoin is actually one of the slower cryptocurrencies due to the relatively small block size (one megabyte per block) and 10 minute average block generation time. Block size is hard coded, but block generation time (TB) is adjusted by changing the difficulty of the hashing puzzle in order to keep block generation time at around 10 minutes.

Transactions speeds can also be slowed down by multiple factors, including network congestion, lack of miners, and any other number of factors. Transaction times reached legendary highs in 2017, during the ICO boom, with users paying exorbitant fees and waiting hours for their transactions to go through.

Multi-signature transactions

Multi-signature addresses are a type of address associated with more than one private key. In order for any transactions to be issued by the address, a proportion of the private keys need to sign off. Let's say Alice, Bob, and Charlie all have private keys for a multi-signature 2-of-3 address containing a whole bunch of bitcoin. Charlie decides to steal all the coins, and move to a country with no extradition treaties. However, the address requires multiple signatures - since it's a 2-of-3 address, this means that Charlie needs to get either Alice or Bob to sign off on the transaction in order to make off with the coins. Multisignature wallets can require any permutation of m-of-n, 2-of-3, 9-of-10, or 5-of-5. Transactions can only be sent as long as all the private keys are able to sign the transaction.

Multi-signature wallets are now commonly used by large exchanges as a means of consumer protection. If a hacker wants to steal the private keys to a wallet and send the bitcoin inside to their own address, they need to work quite a bit harder.

1.2 Bitcoin: The Good, The Bad, and The Ugly

The Good

Deflationary

Inflation, or the decline in the purchasing power of most currencies, is something we're all unfortunately familiar with. Over time, the same amount of money tends to buy less and less. One of the reasons people are so excited about Bitcoin is because it is billed as a deflationary currency. With only 21 million coins in total, Bitcoin has a fixed

liquidity cap. Once all the coins are mined, the lack of new supply theoretically means that the purchasing power of a given bitcoin will increase.

Transparent

Bitcoin is inherently transparent due to the nature of the blockchain. Every transaction ever made, from the genesis block to now, is visible to the public. Since blockchain transactions are immutable, it's possible to get a complete record of Bitcoin's history, including all wallet addresses and the transactions they take part in. This is one of the reasons why laundering money via Bitcoin can be a huge pain, with criminals frequently getting busted when they try to cash out.

Financial freedom

Move money across borders with ease, get around capital controls. Big

hypothetical is if there's a run on the bank and you can't get money out. Popular in countries with unstable currencies. Gives you a degree of control from having spending habits analyzed, with loans that don't impact credit scores with P2P lending. It's when you try to convert Bitcoin into fiat that regulation comes down on you.

Pseudonymity

Bitcoin is frequently mischaracterized as being anonymous. This is what helped earn its colourful reputation as internet money for buying drugs and assassinations. While this is mostly sensational, Bitcoin has been used for certain purchases because it's possible, with some work, to divorce your identity from your Bitcoin transactions.

Since Bitcoin is completely transparent, it's possible to see where money is going,

and often for what purposes if the destination wallet is identifiable. Bitcoin doesn't offer total anonymity, but it's more anonymous than a traditional bank.

Revolutionary

Bitcoin was the first fully functional, widely adopted currency. Without Satoshi Nakamoto's white paper, the crypto industry as we know it wouldn't exist. Borderless, a way to send money across state borders. It disrupted the status quo and introduced blockchain technology to the world.

Very secure

Bitcoin is itself fairly secure. Aside from one incident in 2010 that was quickly mitigated, Bitcoin has never been hacked. [\[16\]](#) Bitcoin is decentralised, distributed over tens of thousands of nodes across the

world. Even if one node is hacked, the network itself will keep running. One theoretical attack on the Bitcoin network is called a 51% attack. If someone gains control over more than half of the Bitcoin network's computing power, or mining hash rate, they can prevent new, valid transactions from gaining confirmations, and gain the ability to double-spend coins.

One of the major protections against vulnerabilities like 51% attacks and fraudulent confirmations is the sheer scale of the Bitcoin network. Due to the protocol's construction, miners are incentivized to keep working for the good of the network as a whole.

Total ownership

Let's say you have money in an online banking service. One day, out of the blue, you're locked out of your funds. You call customer service, send frantic emails, and

even tweet at the company. No dice. Your money is inaccessible, and may as well be gone for all the good it's doing you. This is a common complaint for users of services like PayPal and Venmo. With Bitcoin, the coins you have in your wallet (that you control the private keys for) are yours. You're the only one responsible for them. Of course, this also means that if you fall victim to a scam, no one is going to help you. With great power comes great responsibility, as they say.

Censorship resistant

It's a fact that private companies and governments can interfere in digital fiat payments. Since Bitcoin is blockchain-based, it is decentralized by design. It would be extremely difficult for anyone to censor a transaction.

Entries into the Bitcoin blockchain are immutable - once they're there, they can't be changed or removed. Once a transaction has been added to the ledger, it's nearly impossible to change or delete it.

The blockchain is not owned by a single entity. No state or entity can prevent someone from transacting on the Bitcoin blockchain.

The Bad

Volatility

As popular of an asset as Bitcoin is, its notorious volatility can unnerve cautious investors. Bitcoin is designed as a deflationary asset that increases in value over time. However, regulatory crackdowns and consumer uncertainty have led to rapidly fluctuating prices.

Non-revocable

When you send a Bitcoin transaction, you *cannot take it back*. When they're gone, they're gone. Bitcoin has no customer service, and it is impossible to Karen the blockchain. This is the basis for Bitcoin.

Uncertain future of regulation

In the early years of Bitcoin, people cherished a romantic notion that it was a foolproof way to squirrel money away from prying governments. It was nontaxable and impossible to regulate, they said. A great way to regain sovereignty over your assets, they said. There are two things that are certain in life, and Bitcoin users can't escape taxes. Or regulation. Several countries have banned Bitcoin outright, while the rest of them are scrambling to figure out how to tax and regulate it. There's no way to tell

what the future holds for Bitcoin, legally speaking.

Revolutionary technology

It's a brave new world for crypto users, which can be both good and bad. The lack of precedent is what makes Bitcoin exciting for so many people, and has helped kickstart the crypto revolution. Bitcoin users are definitely on the frontier of something big. Unfortunately, the ecosystem sometimes resembles a saloon in the Wild West during a whiskey-fueled brawl. This was especially apparent during the ICO boom of 2017, when lack of regulation and scruples lead many to get burned. No one can tell what happens next. Prescient and savvy investors stand to make a lot of money, but plenty of people get distracted by fool's gold.

User-hostile tech

While a cornucopia of services offer a simplified experience, users often need to pay high fees and relinquish control over their funds to access easy mode. For those looking for more of a say on their funds, things can get complicated quickly. A typo during a transaction can send your coins hurtling off into the void, never to be seen again. Since Bitcoin transactions are irreversible, every action just seems a little bit more risky. Getting used to the addresses and QR codes can take a bit, and public and private keys are not intuitive to users.

The Ugly

Crime and risk

Contrary to popular belief, the proportion of Bitcoin transactions connected to illegal activity is relatively small.^{[\[17\]](#)} That's not to say that Bitcoin users aren't

at risk. An entire industry has sprung up around relieving unsuspecting people of their bitcoins. There's bitcoin stealing malware, phishing scams, Twitter scams, investment scams, spear phishing, malicious copies of wallet software, malicious copies of wallet hardware, and phishing. If there's a way to steal bitcoins, someone has thought it up and implemented it in a very clever way. Users are faced with an enormous responsibility of keeping their coins safe.

Environmental impact

There's no real way around it: Bitcoin mining is a significant source of carbon emissions. The Cambridge Bitcoin Electricity Consumption Index states that Bitcoin accounts for 0.31% of the world's energy consumption, using approximately 67.72 Terawatt hours. Put into context, that's more than the entire country of Austria.^{[\[18\]](#)} Researchers writing in the

journal Climate Risk Management argued that the impact of the Bitcoin network on the environment warranted the imposition of a carbon tax.^{[\[19\]](#)}

Part 2: How to Get Started with Bitcoin

2.1 Getting Started with Bitcoin

In this section, we'll go over everything you need to know to get started with Bitcoin. We'll cover buying and storing bitcoin, basic security tips, and a few other fun things.

Before you get started, it's important to do the due diligence and think about how you're going to use Bitcoin. Do you want to use it as an investment? Buy weird stuff on the Internet? Learn more about how it works? Whatever you plan to do with it, it's a good idea to have a plan in place before you start buying loads.

There are two major ways to purchase bitcoin: through an exchange, or via private sale. Most people purchase and trade cryptocurrency with the help of cryptocurrency exchanges. These entities allow people to exchange fiat currency for crypto, and different types of crypto for each other. Almost all exchanges are available

online, although there are frequent geographic restrictions for their use due to differences in regulation around the world. While a few do operate brick and mortar storefronts, this has become increasingly unusual.

Getting started on an exchange

In this section, we'll cover different types of exchanges, guidelines on choosing the right one for you, and best practices to make sure your exchange experience is safe.

If there's one thing the world doesn't lack right now, it's cryptocurrency exchanges. There are well over 1000 cryptocurrency exchanges in existence.^{[\[20\]](#)} How can you choose one that works for your needs? Before you pick which exchange you want to use, it's a good idea to think about what factors are the most important. We've included a few parameters to think about while choosing an exchange.

Centralized vs. Decentralized

There are three main types of exchange: centralized exchanges, decentralized exchanges (DEX) and hybrid exchanges.

Centralized exchanges

The exchanges you've most likely heard of before, such as Coinbase and Binance, are all centralized exchanges. They also tend to be the most commonly used by cryptocurrency investors. Centralized exchanges often act like traditional banks and stock exchanges, providing financial services to users for a fee. On top of network transaction fees, they often charge a commission on trades.

While Bitcoin was designed as a decentralized utility, many consumers prefer the benefits that accompany centralized services. Centralized exchanges act as a middleman and provide liquidity. Users

generally put their funds (either fiat or crypto) into the care of the exchange. When they place a buy or sell order, the exchange is responsible for finding a seller or buyer to match. It's often more convenient than hunting down a suitable buyer or seller yourself. However, convenience almost always comes at a premium.

Centralized exchanges also require a lot of trust from their users. When storing crypto on a centralized exchange, users do not control the private keys associated with the crypto. It's vital to consider the security of the exchange when choosing one.

Decentralized exchanges

Decentralized exchanges, commonly referred to as DEXs, follow the original ethos of Bitcoin by cutting out the middleman entirely.

DEXs are usually permissionless, which

means that anyone can access and trade directly without intermediaries. The DEX enables users to carry out peer-to-peer transactions.

How do transactions typically work on a DEX? When Alice places an offer, it usually goes to a *smart contract*. Smart contracts are a type of protocol that can self-execute, self-verify, and self-enforce contracts. The terms of the contract are written into code itself, and contained within a blockchain network.

Alice's offer is submitted to the smart contract. Bob places a bid by submitting a transaction to the smart contract, which then matches buyer and seller and executes the trade.

Decentralized exchanges have a few advantages over centralized exchanges. Since they do not usually take custody of customer funds, they have a lower risk of hacks. The transactions are also more anonymous, since

exchanges often don't require users to conform to KYC and AML regulation. Users keep control over their crypto and private keys, and exchanges are fully transparent and easily audited.

There are also a few disadvantages that come along with using decentralized exchanges. They can be much slower than centralized exchanges. The fact that DEXs don't usually enforce AML or KYC legislation puts them under increased scrutiny from regulatory bodies. There have historically been liquidity problems, and trading volume on DEXs relatively low compared to that of centralized exchanges.^{[\[21\]](#)}

Geographic and currency restrictions

Exchanges tend to have geographic restrictions based on the rules and regulations of different countries. Exchanges also have limitations on the type of fiat currency they accept. Check to make sure that your target

exchange works in your country, and accepts your currency. While you can *technically* use a VPN to access exchanges that aren't legally allowed to transact in your country, this is rarely worth the potential trouble.

Fees

This is the real kicker. Exchanges need to make money somehow, and a lot of them are raking in the dough by charging high fees on top of every crypto transaction. Yes, this is often in addition to the miner fee. There is a trend where the nicer and easier to use the exchange is, the more expensive the fees get. Always make sure to go over the different fee schedules. Fees can vary depending on the type of fiat, trading volume, method of purchase, etc. Read the fine print to avoid any nasty surprises.

If you're planning to make frequent transactions or do any kind of trading, it pays to find an exchange with a preferential fee

rate. Many will offer special discounts and promotions, so keep an eye out.

Liquidity

Bitcoin has had a few liquidity crises over the years, often due to bubbles bursting or major exchange hacks. During those times, people were unable to withdraw funds from exchanges. For this reason, you'll want an exchange with high liquidity. This is generally measured by 24-hour trading volume. The bigger the number, the greater the liquidity.

Customer support

Trying to get customer support from a crypto exchange is like trying to get therapy from your dentist; almost always unsatisfactory. Standards range from bad to criminal. Still, it's worth it to research which exchanges have semi-decent customer service. If

something goes wrong with your account, they're the ones you're going to have to talk to.

KYC and AML compliance

These days, your average Bitcoin exchange transaction is as far from anonymous as you can get. After the 2017 bubble burst, regulators took notice of the rampant scams and gleeful tax dodging that characterized the crypto ecosystem. Exchanges were pressured to comply with KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations.

What this meant for users is that they were required to produce extensive documentation (passport, proof of address, photo of face, etc.) to prove that they weren't using their crypto to commit a crime. If you want perfect anonymity, look for exchanges that aren't KYC compliant. If you're looking for insurance or consumer protection, stick with

regulated exchanges.

Ease of use

If you don't feel confident about your technical ability, try to find an exchange with a user-friendly interface. Bitcoin transactions by themselves are notoriously difficult to parse and user-hostile. If you're worried about messing up when you start out, it's worth it to pay higher fees for an exchange with smooth user experience.

If you're looking to jump right in and start trading, it pays off to find exchanges with rewards schemes, volume-based discounts, and low trading fees.

There are many ways to buy bitcoin. In this book, we are mainly concerned with exchanges. However, there are other options, including meeting someone in person. You should generally avoid telling strangers that

you are going to show up somewhere with mounds of cash and/or bitcoins. Only transact in bitcoins if the counterparty is someone you know and trust. There have been many reported thefts, some violent, associated with this method of exchange.

Safety first!

Bitcoin related scams are on the rise. Where there are large concentrations of money, there is crime. As you get started, it's difficult to tell what's legit and what's not. When money is riding on your ability to assess threats, things get stressful. We've compiled a list of common hacks and scams to look out for, in addition to security tips vetted by experts.

One of the best ways to fend off attacks is to download software updates. Make sure that all of your systems are operating on the latest release. If systems are out of date, they can be vulnerable to attacks.

Hacks and scams: an overview

Fake giveaways

No one wants to give you free money. This seems fairly common sense, but scams where people impersonating celebrities ask for a small sum in return for a larger one are surprisingly successful. The *only* plausible scenario where someone would want to give you free money is if an emerging altcoin is doing an airdrop. Absolutely no one wants to give you free bitcoin. If they say they do, run in the opposite direction.

Phishing

In the world of cybercrime, phishing is a tried and true standby. Phishing refers to an attack where someone entices people under false circumstances to give up personal information that can then be used for nefarious purposes. There are many different

types of phishing attack, but a common vector is via email.^[22]

Customers of the reputable hardware wallet service Ledger were targeted by phishing attacks in 2020. An overview of the case proves that phishing attacks can be incredibly well thought out, elaborate, and creative. Attackers registered domain names that were incredibly similar to the official site, ledger.com.^[23] They then created websites identical to the Ledger site, and sent urgent sounding emails to customers requesting that they enter their 24-word recovery phrase. Once the attacker has access to the phrase, they can immediately drain all funds associated with the wallet.

Always make sure to check the sender's address for misspellings, and don't click on any links unless you're completely satisfied that they have been sent by a trusted source. Try hovering over a link before clicking it to see where the link goes to. Don't open email

attachments unless you trust the sender, as they can contain malware.

Fake exchanges

People will go to great lengths to defraud others, up to and including creating entire fake exchanges. These exchanges offer incredibly competitive prices that lure customers in. Always research exchanges before making a choice. If it looks like they popped out of nowhere, steer clear. Stick to exchanges that have received coverage from reputable sources.

Exchange and wallet hacks

Of course, bitcoin in an exchange is only as secure as the exchange itself. The cryptocurrency ecosystem has a long and fascinating history of heists, hacks, and general bad behavior. We'll cover that a bit later in the book.

Blackmail

Scammers often send emails claiming that they have compromising information, photos, or videos about you. They usually threaten to send the material to all of your contacts unless you pay up via cryptocurrency.

These emails frequently contain user passwords to add weight to the threat. Passwords are often leaked when websites get hacked, so the scammer doesn't necessarily have access to all of your accounts (unless you reuse passwords, which we'll talk about later.)

Almost all of the time, these scammers have no information about you, and are instead relying on you to go into a blind panic and pay up. It's best practice to report the email as spam and then ignore it.

Pyramid / Ponzi schemes / Investment scams

If someone promises you a high-yield investment in return for something, whether that's recruiting new users or an upfront deposit, it's probably a scam. The crypto ecosystem is rife with investment scams as ill-informed investors fall for get rich quick schemes.

Be wary of cold callers or internet pop-up ads that promise fast and highly profitable returns on an investment with low risk. If it sounds too good to be true, it is.

Ransomware

Ransomware typically refers to a type of malware that blocks or encrypts access to a device unless you pay a ransom, often in bitcoin. With ransomware, the important thing is prevention. If it's already happened, you should probably consult a professional. Always be cautious about what you download, and make sure that all applications are legitimate. If an application requests

administrator access, quadruple check it.

Safety tips

Ok, that's a lot of scams! What are a few steps you can take to make sure this doesn't happen to you?

- Use a password manager! It's highly likely that a website you've logged into has been hacked. Hackers typically sell and dump personal information, including emails and passwords, online. People often reuse weak passwords across sites, allowing hackers to get into multiple accounts. It's better and easier to use a password manager.

With a password manager, you only need to remember one strong password. The rest are automatically generated. This protects you from password reuse attacks.

When choosing a password manager, do your research. Popular ones include LastPass, Dashlane, and 1Password, among others.

The <https://haveibeenpwned.com/> website maintains a database of leaked password and email combinations. Try checking it regularly to make sure that your data hasn't been exposed as part of a breach.

If you're working with large amounts of cryptocurrency in a password-protected account, consider using an offline password manager like KeePassXC for cold storage. This is less convenient but adds an extra layer of security.

Above all, *do not reuse passwords*. Just don't do it. Don't even think about it.

- Exchanges often offer extra security features, particularly two-factor

authentication, or 2FA. 2FA refers to an extra layer of security added to the login process, where the person logging in is required to provide an additional form of authentication. This often takes the form of SMS messages to a trusted phone number, an authenticator app, or a physical security key. Take advantage of every safety precaution offered by exchanges - they're there for a reason.

- Don't keep more than you're willing to lose on an exchange. The reasons for this will be explained later, in our history of exchange hacks. Long story short, if your bitcoin is in a wallet that you don't control the private keys for, it's not really yours. Only keep amounts you're actively trading and willing to lose in exchanges.
- Think carefully about your password reset functions. Exchanges often provide a password reset function for people that have forgotten their passwords. This often

takes the form of a link sent to a trusted email. If the email account associated with the exchange is breached, hackers can reset your password and make off with your bitcoins. Every account trusted by the exchange should be secure, with a great, non-reused password, 2FA, and a security question that cannot be guessed by browsing your social media for 10 minutes.

2.2 Exchange Reviews

Finding the right exchange is important and we want to make sure you have the necessary tools and information to make the best decision for your needs.

Our reviews are based on user testing and extensive background research. During the review process we cover end-user feedback and expert opinions to establish the real

reputation and nature of any exchange.

Information is regularly fact-checked and we consult with crypto security specialists to make sure the exchanges we recommend are in your best interests. There is no single best exchange but our reviews can help users find the exchange that suits their individual needs and situation. We've included abridged reviews of 6 popular centralized exchanges.

In addition to reading our reviews, try to seek out more information on exchanges. Check to see if they've been in the news, or have had any major promotions. Remember, just because an exchange hasn't been compromised at the time of writing doesn't mean that it never will be.

Coinbase

Our rating: 3.8/5

Pros: Only crypto exchange listed in the stock exchange

Strong security and insurance on deposits

High liquidity

Smooth user interface

Cons: Higher fees when not using Coinbase Pro

Limited access to altcoins

Wallets are custodial

Overview: Coinbase is one of the first and certainly one of the best when it comes to the cryptocurrency space. It has a smooth and intuitive platform making it seamless for those new to the world of crypto trading.

This simplicity comes at a high price however as the fees add up quickly, especially if you're aiming to trade regularly.

Coinbase can be used to convert one cryptocurrency to another, or to send and receive cryptocurrency. Traders can view price movement, trends, portfolio summaries, and related industry news.

More recently, Coinbase became the first crypto exchange platform to go public and list on the NASDAQ stock exchange with a total value of over \$90 billion.

Recommended for: Anyone looking for an easy, smooth experience while buying Bitcoin.

Luno

Our rating: 3.8/5

Pros: Intuitive, straightforward platform design that doesn't require any hand-holding,

so Grandma can buy her own BTC.

Easy to set up an account and buy crypto

Makes regulated crypto available to users in developing economies

Cons: Luno is a custodial wallet - you don't

own your keys

- Difficult to access customer support

- Confusing fee structure

- Doesn't operate in the US

- Only 6 coins are offered - BTC, ETH, USDC, BCH, LTC, and XRP

Overview: Luno's strengths lie in its usability. It's an easy to navigate, relatively straightforward crypto exchange that makes it easy for newcomers to jump right in and start investing. Founded in 2013 under the name BitX and rebranding to Luno in 2016, the company has grown to serve over 7 million customers with a team of 400+.

Luno's interface is clean and uncluttered. You can also withdraw your coins, and send them to other wallets. There is a week-long cool down period after enabling the send feature. This is presumably for security reasons, but it ends up being massively inconvenient for the user.

Customer support on Luno is difficult to access and requires digging. Security on Luno complies with the industry standard. Fees on Luno depend on the user's country, and can differ wildly.

Recommended for: crypto beginners who are looking for a functional, straightforward buying process.

Kraken

Our rating: 3.8/5

Pros: Powerful interface with multiple languages

- Perks for high-volume traders

- Extensive security measures

- High liquidity

- Available in the US, India, China, and Brazil

- Listed on the Bloomberg Terminal

Cons: Interface that might confuse beginners

Slow customer service
Slow verification

Overview: Currently the largest Bitcoin exchange in terms of volume and liquidity, San-Francisco based exchange Kraken is a solid fit for experienced users that can take advantage of its high liquidity and advanced trading features. Newcomers will benefit from Kraken's high security and 24/7 customer service as well, though they might be intimidated by the complex interface.

Kraken has achieved the significant milestone of being listed on the [Bloomberg terminal](#), a tool relied on by the world's major financial decision-makers.

Kraken has had its fair share of problems over the years. In 2018, Kraken experienced shutdowns lasting as long as [48 hours](#) to address vulnerabilities, spiking unease among investors. However, Kraken's powerful trading tools continue to appeal to high-powered crypto investors, particularly those

based in the United States.

Recommended for: all types of investors, from beginners looking to buy a small amount of bitcoin to high volume traders.

Gate.io

Our rating: 2.8/5

Pros: IEO Platform, for traders looking to invest in upcoming blockchain projects the

- minute they hit the market

- Extensive investment products

- No deposit fees

- Diverse selection of altcoins

Cons: Terrible security track record and lack of transparency

- Cluttered platform

- No fiat deposits

Overview: Founded in the fall of 2013,

Cayman Islands based Gate.io (formerly known as BTER) currently ranks among the 20 largest exchanges. With 650+ cryptocurrencies, it also boasts one of the most diverse asset portfolios. While Gate.io has suffered several major security breaches, it remains a popular choice among traders for its huge stable of altcoins, sophisticated financial services, and robust rewards program.

Gate.io also loses points for being a crypto-only exchange; users cannot deposit fiat. However, the sheer diversity of the coins on offer lessens the sting. Other than that, deposit and withdrawal are fairly easy, though enhanced security measures mean that it might take a little longer than usual.

Fees are slightly lower than industry standard, and start at 0.2%. While it is a standout for coin diversity, the excessive security breaches and cluttered interface mean that Gate.io is not beginner friendly.

Recommended for: Experienced investors willing to compromise on security for access to a large variety of altcoins.

Crypto.com

Our rating: 3.5

Pros: Planning to become carbon negative by 2023

- Offers derivatives and margin trading

- Traded publicly

- Successful debit card service allows you to spend crypto on daily expenses

Cons: Lackluster customer service

- Can be complex to use

Overview: With a dizzying array of features and slick interface, Crypto.com is an excellent choice for beginner to intermediate users looking to integrate crypto into their daily lives.

Founded in 2016, Crypto.com has made a name for itself by providing users the selling of cryptocurrencies at true cost. Their Visa card was launched in 2018, and is currently available in Canada, the US, Europe, and APAC. With perks that include up to 8% cash back and rebates on Spotify, Netflix, and Amazon Prime, it's no wonder that the Crypto.com Visa Card is the largest program of its kind.

Recommended for: Intermediate to advanced users who enjoy earning rewards and want to start integrating crypto into their daily lives.

Binance

Our rating: 4.2

Pros: User-friendly platform

Large selection of crypto

High trading volume delivers greater liquidity to Binance traders

Cons: Customer support can be slow

KYC compliance can take a long time

Was hacked (big time) in 2019,
causing doubts about security

Overview: Binance is a popular cryptocurrency exchange that was founded in 2017 by Changpeng Zhao (CZ). The platform provides trading opportunities for over 500+ cryptocurrencies, especially altcoins. It supports popular coins such as Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Dogecoin (DOGE), including its own blockchain-based token, Binance Coin (BNB).

The exchange has relatively low fees and an attractive user interface. Security isn't great, as the exchange was hacked badly in 2019. On the plus side, Binance has recorded the largest trading volume of any exchange. Binance is constantly adding more options and financial services.

Recommended for: crypto enthusiasts at any level.

Wallet Encryption

It's all well and good to go buy bitcoin, but the important question is how you're going to store it. There are a few important pieces of wallet terminology to explain, followed by key principles. The important thing to remember is this: if you don't control access to the private keys for your wallet, you are not in control of the bitcoins in the wallet.

2.3 How do Bitcoin wallets work?

Bitcoin, and all other forms of cryptocurrency, are based on a branch of science called *cryptography*. Cryptography is a vast discipline with a very rich history that we will not explain in this book, lest we upset

a cryptographer by omitting their favorite bit.

Cryptography refers to the study of encoding and communicating messages so that they can only be read by the intended recipient. This is a very simplified definition, and again, we apologize to all the cryptographers in the audience.

Cryptography is a fundamental part of our lives, and one of the main reasons that it's possible to use chip payment cards and browse securely on the internet. It's also one of the main reasons the Allies won the Second World War. The brilliant mathematician Alan Turing was able to improve on pre-war Polish methods of deciphering German ciphers, enabling the Allies to intercept and decode Nazi messages. This was enormously influential for the Allied war effort, and possibly shortening the war by 2-3 years.^[24]

Ok, cryptography is amazing. But how did

the crypto in cryptocurrency get there? Bitcoin uses different cryptographic methods to maintain the security and accuracy of its transactions: asymmetric key encryption (or public-key cryptography) and hashing.

We've gone over how blockchains are made of blocks of bundled transactions that are connected to previous blocks by a hash. How does this all work? To explain asymmetric key encryption, we'll briefly explain symmetric key encryption.

Symmetric key encryption

In symmetric key encryption, both sides have a key, or secret code that unlocks the encrypted message. The problem with symmetric key encryption is getting that key to both person A and person B, without someone intercepting the key and eavesdropping on their conversation. Transferring the key is difficult to do

securely.

Let's go through a scenario where Alice wants to send Bob private messages about Eve's surprise birthday party without Eve finding out. Alice decides to use symmetric key encryption, so she needs to find a way to get the key to Bob. She sends it via SMS. Eve is a brilliant hacker with a tenuous grasp on the concept of privacy, and intercepts the message. Now she can listen in on Alice and Bob's conversation while they send encrypted messages to each other. The surprise party is ruined.

It was the weaknesses in symmetric key based encryption that enabled Allied codebreakers to intercept keys and listen in on Axis communications.

Asymmetric key encryption

Bitcoin does not use symmetric key encryption. Instead, it uses something called

asymmetric key encryption, or public key encryption, that solves the problem of key distribution. Bitcoin uses cryptographic signatures for validation, and public key encryption prevents impersonation.

In asymmetric key encryption, the key is broken into two parts - public key and private key. If people have the public key, they can encrypt a message and send it to you, which you can decrypt with the private key. Using a very complicated mathematical formula called Elliptic Curve Digital Signature Algorithm (you do not need to remember this), it's possible to derive a public key from a private key. It's impossible to get a private key from a public key. You can give your public key from all and sundry, but they won't be able to get your private key from it.

With the private key, you can also sign a message, and people with the public key can verify it was you that signed it.

In Bitcoin, your public key acts like a bank account number address, and the private key is the ability to actually spend the money in your account. The problem facing public key encryption is called a man in the middle attack, where someone swaps public keys to reroute a transaction.

Alice wants to send Bob money. Bob sends Alice his public key, but Mallory intercepts Bob's message and swaps her key for his. Alice unknowingly sends the bitcoin to Mallory, who promptly goes on a very long holiday to regions unknown.

That's why the common phrase "trust but verify" exists. Always double-check that you're sending a transaction to the right address, much the same way you would with bank accounts.

Hot Wallets vs Cold Storage

Wallets are defined as 'hot 'or 'cold 'based on their internet connection. Hot wallets are

connected to the Internet in some form, while cold wallets are not. Each has their uses. Hot wallets take several forms: there are desktop wallets, mobile wallets, hybrid wallets, and exchange wallets.

If you download a wallet app or set up a wallet on an exchange, you're creating a hot wallet. Hot wallets are usually easy to use, and great for making quick transactions. The main drawback for hot wallets is security. Since hot wallets are online, they are much more exposed to hackers.

Cold wallets, such as paper wallets and hardware wallets, are not connected to the internet, and are considered a much more secure option. Cold wallets are only connected to the internet when you make a transaction. As a rule, the majority of your bitcoin should be kept in a cold wallet. We'll go over a few different types of wallet

Custodial vs. non-custodial wallets

One of the core tenets of Bitcoin's philosophy is maintaining complete control over your assets in the form of your private key. When you control the private keys to your wallet, it is referred to as a *non-custodial* wallet. You can do whatever you want with that bitcoin whenever you want, and no one can stop you.

When you use a non-custodial wallet, that does mean that you have full responsibility for making sure that your bitcoin is safe. That means backing up your wallet and following security best practices. There is no customer care for bitcoin in non-custodial wallets. There is, however, frequent customer care for bitcoin in custodial wallets.

Cryptocurrency service providers like exchanges often offer *custodial wallets*, a type of wallet where you do not control the private key. There are risks associated with custodial wallet in the same way there are

risks with any situation where someone else controls your money. You need to ask permission to exchange and withdraw bitcoin, and you can be kept out of the wallet entirely. There are plenty of cases where people have been barred from accessing funds stored in custodial wallets forever.

In order to use many exchanges and financial products, you will need to deposit some bitcoin into a custodial wallet. Since you don't control the keys, it's best not to keep more bitcoin on an exchange than completely necessary. Consider bitcoin stored in custodial wallets to be at-risk.

Types of wallet

Mobile wallet

Mobile wallets are a type of hot wallet that typically take the form of apps downloaded on a mobile device. They're portable, convenient, and designed to make

transactions easy and frictionless. There are a few downsides to mobile wallets. If you lose or damage your phone, you could lose access to all of your funds. App stores have also removed wallet services in the past, making it difficult to receive necessary updates to keep your wallet secure.

Mobile wallets are a great choice for storing small amounts of bitcoin you plan to use on the go, but be careful about how much you keep in them.

Desktop wallet

Desktop wallets are run on your computer, and are generally more versatile than mobile wallets. You're generally able to exert more control over your bitcoin. They're often compatible with hardware wallets, allowing you to easily access bitcoins kept in cold storage.

Desktop wallets do have downsides. They're

almost always hot wallets, and are popular targets for malware and viruses. It's also a bit harder to use QR codes, making transactions slightly more difficult.

Browser wallets/web wallets

Absolutely not. If you have too much bitcoin and feel the need to get rid of it immediately, consider sending it to me, the author. Or you could use a web wallet. Up to you!

Hardware wallet

If you have a lot of bitcoin, you'll be keeping it in one of these bad boys. Hardware wallets are typically used as cold wallets, though it's possible to mishandle them enough that they turn into hot wallets. The two respectable brands of hardware wallet are Ledger and Trezor.

What hardware wallets have in security they lose in usability. While hardware wallets are

a safe way to store bitcoins, they can be a pain to use for regular transactions. Also, if you lose it and your recovery phrase, you are out of luck.

Paper wallet

Paper wallets are essentially pieces of printer paper with your private key written on it. If you're the type of person that misplaces bookmarks, bills, and receipts, consider buying a hardware wallet.

Setting up your Bitcoin address

Your wallet will generate this for you. If you have a recovery phrase, write it down on multiple pieces of paper, and store them in different geographical locations.

Your public key, or bitcoin address, is generated from your private key. Normally, when you set up a wallet you will be given both a public key and private key.

Wallet safety

- Update everything. Just like with every other system, you need to update your wallet and keep it current. Go update your computer operating system and browser too, while you're at it.
- If it's online it's not safe.
- Always keep multiple copies of your passphrase in secure locations.

2.4 An Abridged History of Exchange Hacks

In this book, we've cautioned against holding large amounts of money in online exchanges. The reasoning behind that has a long and storied history of crime, skullduggery, and extremely poor choices.

If an institution holds a large sum of money, someone will eventually try to steal some.

The cryptocurrency era has seen its fair share of would-be Bonnies and Clydes. Whether or not thieves are successful mainly relies on a combination of factors: the exchange's competence, the hacker's luck, and some skill.

Extremely attractive targets with insane amounts of money. Bitcoin and cryptocurrencies in general are attractive to criminals because the transactions are irrevocable, and the funds can be laundered. Contrary popular belief, laundering money via crypto isn't easy at all. As KYC and AML legislation becomes more common, hacking exchanges has become significantly more difficult. However, people are still managing, with 1.4 billion in crypto stolen in the first five months of 2020 alone. [\[25\]](#)

Beyond hacks, there are many different ways to lose funds to a crypto exchange. Below are some representative examples of what has befallen exchanges.

Mt. Gox - major incompetence

No discussion of exchange hacks is complete without a reference to Mt. Gox, a hack so large it has become legend. The sheer incompetence of the owner leading to such catastrophic losses makes the Mt. Gox hack the Bitcoiner's equivalent to a campfire ghost story. Mt Gox also stands out as a two-parter, with breaches in 2011 and 2014.

Mt. Gox was founded in 2006 in order to facilitate the trading of fantasy game "Magic: The Gathering Online" cards. Founder Jed McCaleb relaunched Mt. Gox as a bitcoin exchange in 2010, selling the exchange to French developer Mark Karpeles in March 2011. In June 2011, 25,000 BTC was stolen, and Mt. Gox's user database leaked. Famously, the price of Bitcoin dropped from \$17 to one cent after a large BTC transfer.^{[\[26\]](#)}

Mt. Gox proceeded to become even more

successful, at one point processing 70% of the world's Bitcoin transactions.

In February 2014, Mt. Gox paused all bitcoin withdrawals, stating that the issue was due to a bug in the Bitcoin software.^[27] A few weeks later, the exchange wiped their Twitter feed, moved their office, and took the website offline. Leaked documents revealed that Mt. Gox was insolvent after losing 744,408 bitcoins over the span of years. The value of Bitcoin plummeted, dropping 36%, and a major liquidity crisis ensued.

QuadrigaCX - force majeure

At one point, QuadrigaCX was Canada's largest Bitcoin exchange, processing nearly \$2 billion in trades at a high point in 2017. Everything was going well for the exchange, up until founder Gerald Cotten died. With him went all knowledge of the private keys to cold wallets storing a fortune in Bitcoin. Cotten left behind a wife, two Chihuahuas,

and 76,000 clients owed a combined \$215 million in assets. Initially, the story went that Cotten had died and took all access to the exchange's cold wallets with him to the grave. As more details came out, however, it became apparent that Cotten was running QuadrigaCX like a Ponzi scheme, and had misused client assets at will for years. Some even believe that Cotten faked his death in an elaborate exit scam. As of now, there are no solid answers.

Coinbase

In 2019, Coinbase was subject to a chillingly well thought out attack by a professional hacker group known as CRYPTO-3, or HYDSEVEN.^[28] The group spent between half a million to a million dollars to create an elaborate, multi-stage setup using the most sophisticated tools available at an incredible speed. Coinbase's security team narrowly avoided disaster by catching and blocking the attack at the last minute. Had it succeeded,

the hackers could have gained access to billions of dollars worth of customer funds.^[29] Hackers are taking the crypto space seriously, and large exchanges like Coinbase are tempting, high-profile targets.

BTC-e - force majeure (US gov't)

Does the US government count as force majeure? BTC-e was a Russia-based exchange founded in 2011. Thanks to its lack of KYC requirements for users and relaxed approach to regulation, by 2016 BTC-e was the third biggest crypto exchange in the world, attracting legitimate investors as well as criminals looking to launder funds.^[30] The exchange's owner, Alexander Vinnik, was indicted by the US Department of Justice in 2017 on 21 counts of money laundering.^[31] BTC-e was also suspected of being heavily involved with laundering some 300,000 BTC from MtGox. The exchange quickly folded. Another apparently unrelated but clearly connected exchange called WEX was set up

soon after. WEX resulted in another set of scandals involving the Kremlin, the FSB (or FSB impersonators), and further losses.

BTER - not a cold wallet!

When is a cold wallet not a cold wallet? A cold wallet is commonly accepted to mean a cryptocurrency wallet that is not connected to the Internet. Cold wallets are conceptually much more difficult to hack. In 2015, China-based exchange BTER announced that 7,170 BTC had been stolen from cold storage. This puzzled users, leading some to believe it was an inside job. Seeing as the exchange had been hacked the previous year, and would then be hacked twice more after it rebranded to Gate.io, there may be some endemic security problems that haven't yet been dealt with.

So, to cap that off, there are a few key principles to observe.

- Don't put bitcoin that you aren't transacting with in hot storage
- Don't keep bitcoin in an exchange for longer than absolutely necessary
- Never, ever, *ever* share your private keys or recovery phrase. With anyone. Ever. For any reason at all. Unless you want them to steal your bitcoin, in which case go for it.

Part 3: Blockchain 101

3.1 What in the name of God is a blockchain

Blockchains are distributed ledger technology. In this section, we'll go over what that means, discuss the benefits and drawbacks of blockchain-based applications, and outline how you can use blockchain analysis to your advantage.

Ok, what is a distributed ledger?

How does everyone know that the same bitcoin hasn't been spent twice? Bitcoins are represented only as transactions, and have no physical form. We know who owns which bitcoins because there is a public ledger with records of every bitcoin transaction ever made. Bitcoin's proof of work, where miners compete to solve math problems and choose the next block, acts as a consensus mechanism. All the nodes and miners need to agree on what the next block is going to be.

Once a block has been appended to the blockchain, it and all the transactions it contains are there permanently. Blockchains are *immutable* - once data is on there, it cannot be altered or removed.

In order to validate transactions and blocks, nodes and miners need to have a full and up to date copy of the Bitcoin blockchain accessible. There are upwards of 11,000

nodes active worldwide at the time of writing.

[\[32\]](#) Full copies of the blockchain are distributed around the world.

One way of understanding the blockchain is by conceptualizing it as a spreadsheet. After all, all blockchains are databases (though not all databases are blockchains). This spreadsheet is publicly viewable, but no one can remove entries. Anyone can suggest a new entry, but it needs to be checked and verified before it's added to the spreadsheet. Thousands of people have constantly updated copies of the spreadsheet. If someone who hated spreadsheets decided to take it offline, they would be faced with the steep challenge of finding and shutting down every single server that hosted the spreadsheet.

Bitcoin was the first example of a working blockchain, but Bitcoin is not the blockchain - it is a protocol that runs using blockchain technology. There is no such thing as *the* blockchain, in the same way as there is no

such thing as *the* computer, *the* postal service, or *the* pizza joint. There are many computers, postal services, and pizza joints, all of which are unique and distinct entities.

3.2 Blockchain Pros and Cons

What are the benefits of blockchains?

A (sort of) trustless system

Most traditional payment systems rely on some form of trusted intermediary, whether that's a bank, a broker, or a credit card company. Trust is usually reinforced by the institution's reputation. Some commentators have said that Blockchain technology was created as a response to the wave of mistrust in financial institutions that swept the world after the 2008 economic crisis.^{[\[33\]](#)}

In contrast, blockchains are described as trustless, since there is no need for an intermediary. Instead, trust is placed in the

protocol, which in the case of Bitcoin is open source and easily auditable. The system is predictable and regulated, and can be relied on. A distributed network of nodes verifies transactions and reaches consensus on a peer-to-peer basis, with no third parties.

Blockchains also offer economic incentives for honest behavior. It is profitable to provide network security, act in the best interest of the many, unprofitable to go against it. The reasoning is that people can be trusted to act in their best interests, and blockchain technology tries to engineer a situation so the best interest of the individual is the best interest of the many.

Open and transparent

The Bitcoin blockchain works because every single transaction is verifiable and visible. Despite the anarchic leanings of early Bitcoiners, blockchain technology is a

valuable tool for law enforcement.

Tamper-resistant

Every block has a type of digital fingerprint, called a hash. It provides proof that a miner earned the right to create a new block, and takes a lot of computing power to create. It also acts like a wax seal on a letter. The cryptographic tools used by the Bitcoin blockchain ensure that altering an entry in any way invalidates all preceding entries.^[34]

If the block is altered, a new hash is generated. In order to verify whether a block is legitimate, all you need to do is check the hash on the block in question with the same block on a different ledger. Same hash? It's the real deal. It's also difficult to change entries in the ledger retroactively, since that would then change the hash for every subsequent block.^[35]

Efficiency

In traditional financial systems, there are numerous expensive, error-prone, and time consuming processes that result from having multiple records. Thin confirmations, actualization of volumes, and all the different forms of reconciliation. Companies are dealing with greater demands for reporting and transparency, which in turn requires meticulous records. Some blockchain proponents argue that a single shared ledger radically increases efficiency.^[36]

Drawbacks of blockchain

Residual points of centralization

Every node requires a copy of Blockchain software to in any way interact with the system. While there are upwards of 11,000

nodes validating transactions and confirming blocks, nearly 95% of them use the same software - Bitcoin Core. The Bitcoin Core developers hold quite a bit of influence over the network.

Bitcoin mining has also become less decentralized over the years. People now use a specific type of hardware, called an ASIC (Application Specific Integration Chips), which is more efficient at crunching hashes than a general-purpose computer. Bitcoin mining now has a barrier to entry in the form of specialized, expensive hardware. [\[37\]](#)

Miners also rarely operate alone. In order to maximize profits, miners join mining pools. As a result, large, centralized mining organizations now control a startling amount of the Bitcoin network's hashing power.

As we discussed previously, one theoretical threat to the Bitcoin network is called the 51% attack. If a group of attackers gains

control of more than half of the network's mining power, they would be able to prevent new transactions from gaining confirmations. They would be able to halt payments between users and reverse transactions completed while they were in control of the network, enabling them to double-spend coins.^[38]

Will it scale?

With the number of transactions per month growing exponentially, the Bitcoin network is facing a scalability problem. The network is limited by the hardcoded size of blocks, and 10 minute block creation time. The average transaction processing speed is between 3.3 and 7 transactions per second. If the network gets too clogged, transactions can slow to a crawl. Ironically, the more Blockchain succeeds and is adopted, the more urgent the scaling problem has become.

Part 4: Bitcoin in the Real World

4.1 Actually Buying Stuff with Bitcoin

In this section, we'll walk you through how to use your Bitcoin, whether as a currency or

an investment, without breaking any laws. We'll go over how to use Bitcoin to purchase pretty much whatever you want through a variety of ways. Then, we'll take a very quick look at Bitcoin as an asset, going over the pros and cons of using it as an investment vehicle.

Finally, we'll make a date with The Man to discuss rules, regulation, and taxation of Bitcoin across the world.

Actually Buying Stuff with Bitcoin

As with any currency, Bitcoin can be exchanged for goods and services. At this point in time, the number and type of those goods and services is more or less infinite, with difficulty levels ranging from trivially easy to very involved.

At this point, it's possible to pay with Bitcoin online and in brick and mortar stores. Just be warned: if you pay in person with Bitcoin,

you might need to wait for a bit for the transaction to get confirmed enough times.

Paying with Bitcoin online is usually very straightforward. Retailers will either provide a wallet address, a QR code, or route you to a payment server. Popular Bitcoin payment services include BitPay, CoinGate, Flexa, and Coinbase. Paypal has recently started to support Bitcoin payments for customers in the U.S., with the exception of Hawaii residents.^{[\[39\]](#)}

Payment processors generally comply with KYC regulation, and demand that users create an account and submit documentation. If you're looking for a more anonymous experience, stick to P2P transactions.

Plenty of retailers accept direct Bitcoin payments. We've included a non-exhaustive list below:

Cars: BitCars, AutoCoinCars
Private jet: Aviatrade, PrivateFly,
GlobeAir
House: Bithomme, cryptocurrency
REITs
Socks: Mt.Socks
VPNs: NordVPN, Surfshark,
ExpressVPN, Cyberghost and ProtonVPN
Flights: CheapAir, Travala
Watches: BitDials
Gold: Bitgild, European Mint
Vidya: Xbox, Playstation
Art: Sotheby's, Singulart, Maecenas,
Crypto Emporium
Domain names: Namecheap, monovm,
Domains \$ Bitcoins
Servers + hosting: server room,
clouviper, coin.host
Tech: Newegg, Microsoft, Rakuten
Charities: The RNLI, Unicef, American
Cancer Society, American Red Cross,
Save the Children, National Society of
Black Engineers, Friends of Notre-Dame
De Paris, and hundreds more

Food and drink: Starbucks (via app),
Whole Foods, some Subway,
Lieferando.de

Gift cards

If you can't buy something directly with Bitcoin, you can almost certainly buy a gift card with Bitcoin and then buy it. Popular gift card sites include Gift Off, BitRefill, Purse.io, and Gyft.

Debit cards

More and more exchanges are starting to offer debit cards. Debit cards convert your crypto to fiat live, while others have an app where you top up the card with Bitcoin.

Every exchange has a unique offering. Exchanges that offer debit cards include Crypto.com, BlockFi, Coinbase, BlockCard, Wirex, Nuri, and Cryptopay.

Investment

Some investors would be horrified at the thought of buying a coffee with Bitcoin. These are generally the types who believe that it has the most value as a speculative asset. The cautionary tale is Bitcoin Pizza Florida Man. He famously spent 10,000 bitcoins on a pair of pizzas. At the time of writing, those pizzas would be worth a cool \$342 million. Thankfully, the guy himself has no regrets, and is happy to be a cultural icon. [\[40\]](#)

Bitcoin's status as a speculative asset is controversial. Cryptocurrency prices are notoriously volatile, and Bitcoin is no exception. Regulatory crackdowns can cause value to plummet, as evidenced by market response to China's repeated moves to squash cryptocurrency use within the country. [\[41\]](#)

Proponents argue that Bitcoin is a good store of value due to its widespread social adoption and recognizable brand on top of its built in

security.^[42] German funds aimed at institutional investors have been granted the ability to invest in crypto, signalling increasing acceptance of Bitcoin from the financial sector.^[43] Goldman Sachs has stated that Bitcoin is a new asset class entirely.^[44] Investors continue to flock to Bitcoin, attracted by its verifiable scarcity and use as a hedge against currency debasement and inflation. In a report from Morgan Stanley Chief Investment Officer Lisa Shalett summarizes the growing positive attitude towards Bitcoin:

“For speculative investment opportunities to rise to the level of an investable asset class that can play a role in diversified investment portfolios requires transformational progress on both the supply and demand sides. With cryptocurrency, we think that threshold is being reached. A firming regulatory framework, deepening liquidity,

availability of products and growing investor interest—especially among institutional investors—have coalesced.”[\[45\]](#)

Detractors say that cryptocurrency speculation is a bubble driven with an outsized appetite for energy that is hastening the climate crisis.[\[46\]](#)

Investing in Bitcoin - the pros

Diversifying your portfolio

No one wants to put all their eggs in one basket, and investing in Bitcoin is a great way to diversify your portfolio.

Capital appreciation

When you take a step back and look at Bitcoin’s history, the gains have been astronomical. Many investors buy and hold on to Bitcoin in the hopes of realizing capital

gains. One important piece of Bitcoin lingo to note: if you see someone on a forum asserting that they plan to “hodl” their bitcoin, the spelling is deliberate. Hodling is a term derived from a very popular meme, and refers to the enthusiasm many have for keeping a tight grip on their bitcoin.

Trust no one

When you buy Bitcoin, you don’t need to put your faith in anyone, or trust some middleman to buy shares on your behalf. You can be assured that your assets exist and are actually available.

Cons

Risky Business

The greater the risk, the greater the reward, and Bitcoin is a deeply risky investment, primarily due to its volatility. In the early months of 2018, many investors lost big after

the price of Bitcoin plummeted from nearly \$20,000 to \$6,000. Investors were stung again in 2021. Bitcoin had rallied to an all-time high of \$63,000 before dropping down to \$30,000.

Regulation risk

It's impossible to know what the regulatory future of Bitcoin holds. It's entirely possible that you'll wake up tomorrow to find your government has outlawed holding and transacting with crypto. This has happened to people around the world, most notably in China. The risk is there, so keep an ear to the ground and pay attention to government discussions on cryptocurrency.

Tax risk

Like regulation, crypto tax is a difficult variable to predict. The only sure thing is that governments will find a way to tax it. If you want to invest heavily in Bitcoin, it's in your

best interest to work with an accountant who understands the tax implications of crypto in your country.

4.2 Bitcoin Around The World: A Regulatory Approach

Every country has its own approach to regulating cryptocurrency. We've included an overview of the regulatory environments in a few countries. The parameters we include are institutional acceptance, exchanges and wallet availability, government regulation, DeFi acceptance, financial services, transparency, ease of spending crypto, and the participation of major banks in crypto.

A few important things to remember:

- Keep records
- Be aware of tax implications
- Find out how cryptocurrency is regulated in your country

Australia - 7.9/10

Dimension	Score	
Institutional acceptance	8/10	100%
Exchanges & Wallets availability	8/10	100%
Government regulation	9/10	100%
Defi acceptance	7/10	100%
Financial services	8/10	100%
Transparency	8/10	100%
Spending crypto	8/10	100%
Banks activity in crypto	7/10	100%

--	--	--

Aussie based investor? Trading cryptocurrencies such as Bitcoin is legal and regulated by the Australian Securities and Investments Commission (ASIC). The country has a very progressive attitude to crypto and a large number of institutions keen to look into the advantages of the all-important technology behind it. You'll need to pay tax on your gains, of course, and there are a number of well-established crypto exchanges that make it easy and straightforward to buy, sell and invest in Bitcoins (BTCs) and other cryptocurrencies.

Australia has taken a highly positive approach to regulating crypto exchanges for consumer protection and harnessing the advantages of blockchain technology in the mainstream financial sectors. The country also has a thriving crypto investor base with a

high number of ATMs.

Country facts

- Total Population - 25.5m
- Number of crypto owners - 857.6k
- Percentage of the population owning Crypto - 3.4%
- Residents crypto interest country rank - 12

Services

- # of exchanges based in Country - 11
- # of bitcoin nodes based in Country - 101
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$55m
- # of ATMs - 54

Belgium - 7.9/10

Dimension	Score	World Rank
Institutional acceptance	8/10	14

		cc
Exchanges & Wallets availability	8/10	A pr
Government regulation	8/10	R V
DeFi acceptance	5/10	N
Financial services	8.5/10	G ar
Transparency	8.5/10	Pe re
Spending crypto	9/10	V A
Banks activity in crypto	8/10	L di

Belgium isn't all chocolates and chintz - it's also coming on as a bit of a crypto hub, with a growing number of crypto investors and bitcoin ATMs. All the major exchanges are able to offer their services and there are a developing number of retailers and online

retailers who'll accept bitcoin payment. You'll need to pay tax on your gains if you buy and sell cryptocurrency but by and large you'll be able to buy, sell and trade, once you've opened an account and there are plenty of specialists around to help if you want advice on tax and investing matters.

Belgium is keen to adopt aspects of blockchain and its banking sector wants to harness the consumer demand from crypto trading and investment. One of its largest banking and insurance groups is also exploring a cryptocurrency for internal use and there is a growing crypto retail acceptance.

Country facts

- Total Population - 11.6m
- Number of crypto owners - 273k
- Percentage of the population owning Crypto - 2.4%
- Residents crypto interest country rank - 16

Services

- # of exchanges based in Country - 0
- # of bitcoin nodes based in Country - 30
- Bitcoin Trading Volume on Online

Exchanges in 2020 - N/A

- # of ATM's - 42

Canada - 7.9/10

Dimension	Score
Institutional acceptance	8/10
Exchanges & Wallets availability	9/10
Government regulation	8/10
Defi acceptance	7/10
Financial services	8/10

Transparency	8/10	1
Spending crypto	7/10	0
Banks activity in crypto	8/10	1

Canada is a land of opportunity and enterprise, and crypto is becoming an attractive option to over a million bitcoin holders to date. Regulation is clear and there is tax to pay when you trade and make gains. But hey, The Canadian Revenue Agency (CRA) places crypto assets in the category of property and if you want to trade Bitcoin, there are a number of well-established crypto exchanges that make it easy and straightforward to buy, sell and invest in Bitcoin and other cryptocurrencies. There are a widening number of outlets and services you can spend crypto on, or you can simply invest for gain. Beats lumberjacking!

Canada has many progressive advocates for

crypto and blockchain technology. The central bank has involvement in a digital currency and there is firm regulation and a healthy crypto investment framework.

Country facts

- Total Population - 37.7m
- Number of crypto owners - 1.2m
- Percentage of the population owning Crypto - 3.2%
- Residents crypto interest country rank - 9

Services

- # of exchanges based in Country - 8
- # of bitcoin nodes based in Country - 288
- Bitcoin Trading Volume on Online

Exchanges in 2020 - \$66m

- # of ATM's - 4

France - 7.4/10

Dimension	Score
Institutional acceptance	7/10
Exchanges & Wallets	8/10

availability	
Government regulation	8/10
Defi acceptance	6/10
Financial services	7/10
Transparency	8/10
Spending crypto	7/10
Banks activity in crypto	8/10

A lot of French folk are taking crypto to their hearts with over 3.5 million holders in the country to date. The Government is keen to see where all things crypto lead and although there are very firm rules and regulations for crypto exchanges and services. If you're a France based resident, there are both leading

and home-based exchanges to choose from, with gift card schemes to make spending your cryptocurrency easy. If you want to trade crypto you'll have to pay tax on your gains, but there are rumours that tax on crypto may soon be reduced.

Many French businessmen and thought leaders want France to be at the forefront of all things crypto. The Central bank is also trailing digital currency. Plenty of consumer investment activity and places to spend crypto with very positive lobbying for blockchain progress.

Country facts

- Total Population - 65.3m
- Number of crypto owners - 3.5m
- Percentage of the population owning Crypto - 5.3%
- Residents crypto interest country rank - 44

Services

- # of exchanges based in Country - 3
- # of bitcoin nodes based in Country - 538
- Bitcoin Trading Volume on Online Exchanges in 2020 - N/A
- # of ATM's - 9

Germany - 7.6/10

Dimension	Score
Institutional acceptance	8/10
Exchanges & Wallets availability	9/10
Government regulation	8/10
Defi acceptance	5/10
Financial services	8/10
Transparency	7/10

Spending crypto	8/10	
Banks activity in crypto	8/10	

Looking to grab a kleine piece of the crypto action? Germany is one of the first countries to enable financial institutions to custody crypto assets as a new type of financial service incorporated into the German Banking Act. There is firm regulation and guidance for service providers and with interest rates so low, crypto investing is an attractive option - which is why over 3.5 million residents hold some form of crypto to date. There are plenty of places to spend crypto, and lots of exchanges to choose from.

Germany has taken firm and imaginative action in defining and accommodating the growth of cryptocurrency and blockchain

technology - in part probably driven by negative interest rates on traditional cash deposits and demand-push from investors. The Capital, Berlin, is a hot spot for spending crypto, so all in all Germany earns a 7.6/10.

Country facts

- Total Population - 83.8m
- Number of crypto owners - 3.1m
- Percentage of the population owning Crypto - 3.8%
- Residents crypto interest country rank - 7

Services

- # of exchanges based in Country - 1
- # of bitcoin nodes based in Country - 1,679
- Bitcoin Trading Volume on Online Exchanges in 2020 - N/A
- # of ATM's - 30

Hong Kong - 6.6/10

Dimension	Score	Why
-----------	-------	-----

Institutional acceptance	8/10	Wide regula
Exchanges and Wallets	7/10	Leadi access
Government regulation	7/10	Taxat reasor profes
DeFi acceptance	5/10	No re
Financial services	5/10	Grow
Transparency	8/10	Person tracki
Spending crypto	5/10	High to spe
Banks activity in crypto	8/10	Recen world broke

Hong Kong has a healthy consumer base looking to invest in crypto and a high number of ATMs, over 120 to date. Tax laws aren't

particularly prohibitive - at present, at least - and crypto is seen more as an investing activity rather than a spending activity. There are places to spend crypto and lots of recognised exchanges to choose from - some may even be able to help with your transaction record keeping.

Hong Kong gets a 6.6/10 CoinCub Crypto Rating through wide institutional acceptance of cryptocurrencies and low tax on gains undermined by uncertainty over future legislation and undeveloped retail opportunities for spending crypto.

Country facts

- Total Population - 7,4 m
- Number of crypto owners - 245k
- Percentage of the population owning Crypto - 3.3%
- Residents crypto interest country rank - 28

Services

- # of exchanges based in Country - 25

- # of bitcoin nodes based in Country - 96
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$20.1m
- # of ATM's - 127

Hungary - 7.0/10

Dimension	Score	Why
Hungary is Institutional acceptance	8/10	Increasing
Exchanges & Wallets availability	8/10	All leading and access
Government regulation	9/10	Light. And for near fut
Defi acceptance	6/10	Governmer its advantag
Financial services	5/10	Leading ins
Transparency	7/10	Personal da tracking
Spending crypto	9/10	Well-establ
Banks activity in crypto	4/10	Leading ba

Resident of Hungary and thinking about Bitcoin? You could be in luck - Hungary is quite a friendly place to buy and sell cryptocurrencies with all the leading exchanges and wallets available. There is a fairly open acceptance of all things crypto with a lot of services, goods and products available to purchase with cryptocurrency. In addition to a light tax regime for trading, the government is also planning to reduce tax on trading even more in a move to encourage greater tax compliance - so what are you waiting for?

Hungary has a great deal of crypto owners relative to its population size, there is a keenness for crypto spending and investing with participating exchanges and retail outlets - and the government is planning tax reductions to increase compliance with tax policy.

Country facts

- Total Population - 9.7m
- Number of crypto owners - 131k
- Percentage of the population owning Crypto - 1.4%
- Residents crypto interest country rank - 43

Services

- # of exchanges based in Country - 2
- # of bitcoin nodes based in Country - 29
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$0.2m
- # of ATM's - 52

India - 6.9/10

Dimension	Score	Why
Institutional acceptance	5/10	Uncoordinated
Exchanges & Wallets availability	8/10	Leading names exchanges
Government	3/10	No clear guidance

regulation		
Defi acceptance	5/10	Government loc advantages
Financial services	8/10	Banks have tap
Transparency	9/10	Normal ID requ accounts
Spending crypto	9/10	Established outl
Banks activity in crypto	8/10	Leading banks a promote service

Looking to buy and sell bitcoin and other cryptocurrencies? As a resident of India, you're in good company because to date, there are over 10 million people holding bitcoin and a staggering number of exchanges offering their services, both overseas and home-based ones. Regulation and laws on trading are still very much in a state of flux - but it hasn't stopped consumers wanting to get in on the action.

India has an inconsistent approach to crypto with low institutional acceptance and regulations whilst leading exchanges are all present with banks looking to tap into demand for crypto from consumers that don't have bank accounts.

Country facts

- Total Population - 1.37B
- Number of crypto owners - 10m
- Percentage of the population owning Crypto - 0.7%
- Residents crypto interest country rank - 48

Services

- # of exchanges based in Country - 8
- # of bitcoin nodes based in Country - 16
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$64m
- # of ATM's - 1

Ireland - 7.5/10

Dimension	Score
Institutional acceptance	7/10
Exchanges & Wallets availability	9/10
Government regulation	8/10
Defi acceptance	5/10
Financial services	7/10
Transparency	8/10
Spending crypto	8/10
Banks activity in crypto	8/10

Irish residents rejoice - investing in crypto is legal in the Republic. Crypto trading currently relies on guidance provided by the

Central Bank of Ireland, which is responsible for the regulation of the financial services industry. However, EU directives, money laundering laws bear strongly on crypto trading activity, not to mention standard income tax and CGT laws.

Ireland scores a 7.5/10 for a government open to maintaining the country's financial attractiveness and looking positively at blockchain. Crypto is seen as an investment by many consumers with a growing base of online and traditional retailers accepting it.

Country facts

- Total Population - 4.9m
- Number of crypto owners - 84.7k
- Percentage of the population owning Crypto - 1.7%
- Residents crypto interest country rank - 13

Services

- # of exchanges based in Country - 1

- # of bitcoin nodes based in Country - 36
- Bitcoin Trading Volume on Online Exchanges in 2020 - N/A
- # of ATM's - 22

Japan - 7.8/10

Dimension	Score	Why
Institutional acceptance	8/10	Very to cry
Exchanges & Wallets availability	9/10	All le and a
Government regulation	8/10	Gove high t
Defi acceptance	6/10	Gove advan
Financial services	5/10	Leadi forms
Transparency	9/10	Perso tracki

<u>Spending crypto</u>	<u>8/10</u>	Japan servic
Banks activity in crypto	8/10	Leadi and p

If you're a resident of Japan and thinking of joining the rush to crypto and bitcoin trading you're in a good place. Japan has clear and firm regulations on crypto trading and it is legal and acceptable - if not mainstream - with all the leading exchanges offering their services to help you invest. Taxes are high, but if your gains from crypto are only moderate your tax won't be quite so Godzilla-sized either.

Japan is taking a positive lead on crypto with regulation and guidance. There are plenty of opportunities to invest and spend, with institutions looking at tapping into crypto but trading carries high taxes and penalties for non-disclosure.

Country facts

- Total Population - 126.8m
- Number of crypto owners - 2.1m
- Percentage of the population owning Crypto - 1.6%
- Residents crypto interest country rank - 64

Services

- # of exchanges based in Country - 15
- # of bitcoin nodes based in Country - 108
- Bitcoin Trading Volume on Online

Exchanges in 2020 - \$7m

- # of ATM's - 1

Mexico - 6.6/10

Dimension	Score	Why
Institutional acceptance	6/10	Accepted bu
Exchanges & Wallets	8/10	All leading r

availability		access.
Government regulation	5/10	Light and un
Defi acceptance	4/10	Not yet
Financial services	5/10	Leading inst
Transparency	6/10	Personal data
Spending crypto	9/10	Wide-spread
Banks activity in crypto	4/10	Banks yet to

Are you a Mexico resident thinking about buying some bitcoin or other cryptocurrency? Mexico has a thriving crypto economy where crypto is used by a wide number of the population to facilitate everyday life. Correspondingly there are plenty of outlets with services and products you can buy. Regulation is light and all the leading exchanges are present to offer their services.

Mexico is difficult to score as the population

are enthusiastic users of crypto to facilitate their economic needs, but the establishment has no strategy for advancing crypto at an institutional level.

Country facts

- Total Population - 129.1m
- Number of crypto owners - 3.2m
- Percentage of the population owning Crypto - 2.5%
- Residents crypto interest country rank - 52

Services

- # of exchanges based in Country - 3
- # of bitcoin nodes based in Country - 12
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$23m
- # of ATM's - 13

New Zealand - 5.8/10

Dimension	Score	Why
-----------	-------	-----

Institutional acceptance	6/10	Cryp allow
Exchanges & Wallets availability	6/10	All le of ho
Government regulation	6/10	Light
Defi acceptance	5/10	No li
Financial services	6/10	Inter block
Transparency	6/10	Persc track
<u>Spending crypto</u>	<u>6/10</u>	<u>Cryp</u> <u>inves</u>
Banks activity in crypto	5/10	No re facili

Are you a resident Kiwi? If you're looking to buy or sell bitcoin or other cryptocurrency in New Zealand then there's nothing to stop you. The country accepts crypto trading - and taxes it, obviously - and regulation is light.

Leading exchanges operate but there is not a lot to spend crypto on as it's mostly an investment play by those who buy it and you need to keep records of your deals for the taxman.

Country facts

- Total Population - 4.8m
- Number of crypto owners - 85k
- Percentage of the population owning Crypto - 1.8%
- Residents crypto interest country rank - 21

Services

- # of exchanges based in Country - 4
- # of bitcoin nodes based in Country - 24
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$10m
- # of ATM's - 0

Poland - 7.5/10

Dimension	Score	Wh
Institutional acceptance	8/10	Fav allo
Exchanges & Wallets availability	8/10	All pres
Government regulation	7/10	Tax to o
Defi acceptance	5/10	No
Financial services	7/10	Gro and blo
Transparency	7/10	Per trac
Spending crypto	8/10	Ma AT
Banks activity in crypto	7/10	Gro con nun

As a resident of Poland you can buy and sell

cryptocurrency through a widening number of leading global exchanges - and, even better, taxation rates on your hard-earned gains are reasonable. There are a growing number of outlets that accept crypto with a large number of bitcoin ATMs, over 100, across the country.

Poland scores a healthy 7.5/10 on crypto friendliness with a very positive government outlook and low taxes and a high and growing number of ATMs. Places to spend crypto are expanding, especially within the tourist industry.

Country facts

- Total Population - 37.8m
- Number of crypto owners - 945.3k
- Percentage of the population owning Crypto - 2.5%
- Residents crypto interest country rank - 39

Services

- # of exchanges based in Country - 4

- # of bitcoin nodes based in Country - 44
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$4m
- # of ATM's - 112

Romania - 6.3/10

Dimension	Score
Institutional acceptance	5/10
Exchanges & Wallets availability	6/10
Government regulation	8/10
Defi acceptance	5/10
Financial services	7/10

Transparency	8/10
Spending crypto	6/10
Banks activity in crypto	5/10

As with many countries, Bitcoin is accepted and traded legally even if it is not designated as a traditional currency. That said, Romania has a high number of Bitcoin ATMs for its size and a healthy number of retailers willing to accept it, especially in Bucharest.

Regulations aren't fully developed but the good news is tax on trading is relatively low and there's no VAT.

Romania is representative of many countries to crypto with low regulation and institutional uncertainty but with wider acceptance among the population fuelled by low tax on trading.

Country facts

- Total Population - 19.1m
- Number of crypto owners - 423.5k
- Percentage of the population owning Crypto - 2.2%
- Residents crypto interest country rank - 34

Services

- # of exchanges based in Country - 1
- # of bitcoin nodes based in Country - 33
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$5m

- # of ATM's - 90

Singapore - 8.4/10

Dimension	Score	Why
Institutional acceptance	9/10	Very positive. l
Exchanges & Wallets	9/10	All leading nan access plus wid

availability		exchanges
Government regulation	9/10	Clear guidance
Defi acceptance	6/10	Government loan advantages
Financial services	8/10	Leading financial strategies
Transparency	9/10	High requirements for firms and individuals
Spending crypto	9/10	Well-established outlets
Banks activity in crypto	8/10	Leading banks promote services

Singapore has taken crypto to heart and has a very positive outlook towards buying and selling it. There are leading exchanges to choose from with clear regulation and guidance covering financial services generally. Add in well established outlets for spending and you have a country that wants to maintain its position as a financial hub. As

a Singapore resident you might find yourself dipping your toe into the market.

In keeping with maintaining its competitive position, Singapore offers firm but clear legislative guidance with low tax on crypto earnings combined with progressive attitude within the financial sector and lots of retail take-up.

Country facts

- Total Population - 5.6m
- Number of crypto owners - 121k
- Percentage of the population owning Crypto - 2.1%
- Residents crypto interest country rank - 8

Services

- # of exchanges based in Country - 32
- # of bitcoin nodes based in Country - 134
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$11m
- # of ATM's - 10

Spain - 6.8/10

Dimension	Score
Institutional acceptance	7/10
Exchanges & Wallets availability	8/10
Government regulation	6/10
DeFi acceptance	5/10
Financial services	6/10
Transparency	7/10
Spending crypto	8/10
Banks activity in crypto	7/10

Like many European countries, Spain has a wait and see approach to crypto. Nevertheless buying and selling cryptocurrencies is a popular activity for well over a million Spaniards and there is a high number of bitcoin ATMs around the country. There's also some reasonable tax relief on your gains and a number of developed outlets for spending crypto.

Spain, as with many countries, has a groundswell of population and grass-roots organisations willing to advocate greater crypto acceptance and its implications but the Government and its institutions are moving slowly.

Country facts

- Total Population - 46.7m
- Number of crypto owners - 1.2m
- Percentage of the population owning Crypto

- 2.5%
- Residents crypto interest country rank - 18

Services

- # of exchanges based in Country - 1
- # of bitcoin nodes based in Country - 71
- Bitcoin Trading Volume on Online

Exchanges in 2020 - N/A

- # of ATM's - 144

Sweden - 8.0/10

Dimension	Score	Why
Institutional acceptance	9/10	Very positive Krona
Exchanges & Wallets availability	9/10	All leading and access
Government regulation	9/10	Government society
Defi acceptance	6/10	Government its advantages

Financial services	6/10	Leading ins of crypto se
Transparency	9/10	Personal da tracking, hi
Spending crypto	8/10	Has well-es services
Banks activity in crypto	8/10	Leading ba and promot

Cool Sweden is definitely hot when it comes to crypto with a very positive institutional outlook towards cryptocurrency and especially blockchain technology. The country already has plans for a cashless society and a healthy 2.3% of the population have some crypto dealings. There are all the leading exchanges to choose from and developed outlets for spending some of your crypto - but, of course, you'll have to pay a stiff tax on your gains.

Sweden has a positive attitude towards crypto and blockchain potential that runs from the

top down with an openness to a cashless future and numerous crypto trading and spending facilities.

Country facts

- Total Population - 10.1m
- Number of crypto owners - 228.3k
- Percentage of the population owning Crypto - 2.3%
- Residents crypto interest country rank - 24

Services

- # of exchanges based in Country - 2
- # of bitcoin nodes based in Country - 93
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$23m
- # of ATM's - 0

The Netherlands - 7.0/10

Dimension	Score

Institutional acceptance	8/10
Exchanges & Wallets availability	8/10
Government regulation	6/10
DeFi acceptance	6/10
Financial services	6/10
Transparency	7/10
Spending crypto	8/10
Banks activity in crypto	7/10

The Netherlands gets 7.0/10 for its mix of wide cultural acceptance of crypto, equally open to investing and spending crypto unhindered, but with no specific government lead on regulation or strategy. Trading Bitcoin in The Netherlands is well advanced

and the country has a healthy acceptance of Bitcoin and other cryptocurrencies. The country offers plenty of choices when selecting a bitcoin exchange and, as a Dutch resident/user, you can choose from platforms based at home or overseas.

Country facts

- Total Population - 17.2m
- Number of crypto owners - 521.4k
- Percentage of the population owning Crypto - 3%
- Residents crypto interest country rank - 5

Services

- # of exchanges based in Country - 6
- # of bitcoin nodes based in Country - 408
- Bitcoin Trading Volume on Online Exchanges in 2020 - N/A
- # of ATM's - 16

United Kingdom - 6.8/10

Dimension	Score
Institutional acceptance	7.5/10
Exchanges & Wallets availability	9/10
Government regulation	7/10
Defi acceptance	2/10
Financial services	4/10
Transparency	9/10
Moving cross border	9/10
Banks activity in crypto	7/10

Britain's banks aren't particularly enamoured of crypto, but there are plenty of people who

are buying into it - well over 3 million at the last count. Exchanges are available on a large scale along with over 200 bitcoin ATMs at present. Mostly seen as an investment for gain than a spending ploy. Having said that, crypto is easy to spend with a growing number of online retailers. There is also a useful capital gains tax allowance on your initial gains too.

The UK scores a high crypto rating of 6.8/10 thanks to the wide range of crypto services offered and ever-clearer guidance and transparency. As yet, the UK remains more of an investment opportunity for crypto rather than a spending hub.

Country facts

- Total Population - 68m
- Number of crypto owners - 3.4m
- Percentage of the population owning Crypto - 5%
- Residents crypto interest country rank - 19

Services

- # of exchanges based in Country - 53
- # of bitcoin nodes based in Country - 233
- Bitcoin Trading Volume on Online

Exchanges in 2020 - \$[193m](#)

- # of ATM's - 230

United States - 7.6/10

Dimension	Score
Institutional acceptance	8/10
Exchanges & Wallets availability	10/10
Government regulation	7/10
DeFi acceptance	5/10
Financial services	8/10

Transparency	7/10
Spending crypto	8/10
Banks activity in crypto	8/10

As with many things - like aircraft carriers, burgers and film stars, the US does it bigger - and crypto is no exception. Although crypto is still a hot and controversial subject - the last President wasn't exactly keen on it - many institutions see the upside in much of blockchain technology. With over 37 million crypto holders in the US - and a growing consumer demand, the financial sector is looking to embrace crypto fever in some way.

The US gets 7.6/10 for wide consumer acceptance of crypto with the world's leading exchange listed on Wall St and retail banks looking to compete for services, but a

disparate crypto focus from state to state.

Country facts

- Total Population - 331m
- Number of crypto owners - 37m
- Percentage of the population owning Crypto - 11.2%
- Residents crypto interest country rank - 20

Services

- # of exchanges based in Country - 29
- # of bitcoin nodes based in Country - 1,671
- Bitcoin Trading Volume on Online Exchanges in 2020 - \$[1,524m](#)
- # of ATM's - 18,667

Part 5: Glossary

Address: A Bitcoin address is a string of alphanumeric characters that bitcoins can be sent to and from. Bitcoin addresses can be shared publicly, and provided to others that want to send you bitcoin.

Altcoin: Any alternative digital currency to Bitcoin.

AML – Anti Money Laundering regulation. Most governments have some form of this for financial and crypto exchanges.

BTC: An abbreviation of Bitcoin.

Bit: A commonly used unit to designate the subunit of a bitcoin. 1,000,000 bits is equal to one bitcoin (BTC).

Bitcoin: A type of cryptocurrency created in 2009 that uses peer-to-peer technology to facilitate payments.

Block: A record in the blockchain that contains transactions that occurred during a certain period of time, usually about 10 minutes. If the Bitcoin blockchain is like a ledger, then a block can be considered a page in the ledger.

Blockchain: A public record of Bitcoin transactions arranged in chronological order. It acts as the authoritative account of every Bitcoin transaction that has ever occurred.

Bubble: A well worn financial expression to indicate a market where investors are pouring money into a stock or investment opportunity and grossly overvaluing it – usually followed by a market collapse in that asset.

Central Bank: A country's main bank for issuing currency, overseeing monetary policy and sometimes setting interest rates.

Custody/Custodial Services: The service

provided by a crypto exchange or sometimes a bank to take custody of your wallet and conduct cryptocurrency transactions on your behalf.

Cryptocurrency: Any of the so-called digital currencies such as Bitcoin etc. They may be called currencies, but they are not recognized as such by governments in the same way as traditional 'flat 'currency such as dollars, pounds etc.

Cold Storage: The storage of Bitcoin private keys in any way that is not connected to the internet. Common forms of cold storage include hardware wallets, external drivers, paper wallets, and offline computers.

Cold Wallet: A Bitcoin wallet that is not connected to the internet.

Confirmation: A formal agreement by nodes that a transaction or block is valid. Transactions receive confirmations when they

are included in a block. All transactions are considered unconfirmed until they are added to a block, with each additional block serving as another confirmation. The more confirmations a transaction has, the less likely it is to be reversed.

Cryptography: A branch of mathematics that concerns the practice and study of techniques for secure communication in the presence of an adversarial third party. In the context of Bitcoin, cryptographic techniques are used to create secure wallets, sign transactions, and link blocks to each other.

Crypto Exchange: Similar to any trading exchange, such as for shares, but dealing in cryptocurrencies.

DeFi: Short for decentralized finance. Refers to a variety of financial applications that use cryptocurrency or blockchain technology to create services that eschew financial intermediaries.

Double spend: When a malicious user attempts to spend their bitcoin twice at the same time.

Encryption: The process of encoding information so that only the intended recipient can decode and read it.

Flat Currency: This is taken to mean the internationally recognized and accepted traditional currencies issued by governments, such as dollars, pounds euros etc.

FUD: An acronym that stands for Fear, Uncertainty, Doubt. Used in investment contexts to refer to the baseless or exaggerated claims made to induce negative sentiment about assets.

Hodl: An intentional misspelling of the word “hold”, now a shorthand for an approach to cryptocurrency that rejects trading based on short-term price moves.

Hash: 1) A mathematical function that converts any input to an encrypted output of a fixed length. 2) A unique identifier for Bitcoin transactions.

Hash rate: The measuring unit for the processing power of the Bitcoin network. The hash rate is also an important security metric, since more hashing power in the network equals greater security.

Hot Wallet: Any type of wallet that is connected to the internet.

ICO: Initial Coin Offering. A type of fundraising method where investors are allowed to buy into an offering and receive a new cryptocurrency token in return.

KYC: Or Know Your Customer, one form of compliance or regulation that is required of bodies dealing in digital currency.

Miner: A computer that confirms Bitcoin transactions by spending electricity performing tedious and difficult mathematical calculations. Miners are sometimes rewarded with transaction fees and new bitcoins.

Multi-Signature: A bitcoin transaction that requires signatures from more than one key before it can be executed.

Node: A participant in the Bitcoin network that holds a copy of the full Bitcoin blockchain.

Open Source: Any software that is free and open to use, usually stored in a public repository and shared publicly. Anyone can use the code or contribute improvements.

P2P: Short for peer-to-peer. Refers to systems that allow users to interact directly with each other, without the recourse to a third party.

Paper Wallet: A type of wallet where private keys are printed or written on a piece of paper. Considered a type of cold wallet.

Private Key: A string of alphanumeric characters that proves the right of the user to spend bitcoins from a specific wallet.

Public Key: A string of alphanumeric characters derived from a private key. Public keys act as an address, and allow the holder to receive bitcoin.

Quantitative Easing (QE): A monetary policy used by central banks in order to stimulate the economy. Roughly speaking, the central bank buys bonds and share holdings from major investment bodies such as pension funds – these bodies then have the cash to reinvest. Done en-masse it provides a big injection of money into the economy. Referred to by detractors as “printing money”.

SHA-256: Short for Secure Hash Algorithm 256. The specific hash function used by the Bitcoin protocol.

Satoshi: The smallest unit of a bitcoin. There are 100,000,000 satoshis in one bitcoin, so one satoshi = 0.0000001.

Satoshi Nakamoto: The anonymous founder of Bitcoin.

Signature: A mathematical mechanism that allows someone to prove ownership of specific bitcoins.

Wallet: A private key or collection of private keys that enable users to hold and spend bitcoin.

Thanks for reading!

If you enjoyed this book, consider visiting our website at coincub.com, or send us your feedback at contact@coincub.com.

Bite-Size Bitcoin

A pain-free guide to the world's
largest cryptocurrency

ASIN:B09LJ1R1Z4

Authors: *Laurel Murphy, Jon Lea and the
Coincub Team*

Publish Date: August 2021

© Coincub 2021 - Vetted crypto services in your country

All rights reserved - IPOI Reg No. 265792
Marine House, Clanwilliam Place, Dublin 2, Ireland

-
- [1] <https://bitcoin.org/en/bitcoin-core/>
 - [2] <https://bitcoin.org/en/posts/ten-year-anniversary>
 - [3] <https://nakamoto.com/the-cypherpunks/>
 - [4] https://en.bitcoin.it/wiki/Genesis_block
 - [5] <https://arstechnica.com/tech-policy/2013/03/us-regulator-bitcoin-exchanges-must-comply-with-money-laundering-laws/>
 - [6] <https://www.bbc.com/news/av/technology-24756030>
 - [7] <https://www.theverge.com/2013/11/27/5151396/bitcoin-hits-1000>
 - [8]
 - [9] <https://www.japantimes.co.jp/news/2016/03/04/business/teoks-recognizing-virtual-currencies-similar-real-money/>
 - [10]

- [11] <https://www.marketwatch.com/story/nearly-half-of-all-2017-icos-have-failed-2018-02-26>
- [12] <https://www.cnn.com/2020/03/13/bitcoin-loses-half-of-its-value-in-two-day-plunge.html>
- [13] https://en.wikipedia.org/wiki/Bitcoin#cite_note-42
- [14] <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-crime-caveats/#:~:text=%E2%80%9CIn%202020%2C%20the%20i>
- [15] <https://www.google.com/search?q=bitcoin+transaction+speed&sxsrf=ALeKk00wIY47keF3DImqA0&start=0&sa=N&ved=2ahUKEwiE8OORiNLxAhUtU>
- [16] <https://hackernoon.com/bitcoins-biggest-hack-in-history-184-4-ded46310d4ef>
- [17] <https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/#:~:text=According%20to%20an%20excerpt%20for>
- [18] <https://cbeci.org/cbeci/comparisons>
- [19] <https://www.sciencedirect.com/science/article/pii/S22120963>
- [20] <https://blockspot.io/exchange/>
- [21] <https://www.nasdaq.com/articles/decentralized-and-centralized-exchanges%3A-who-will-win-the-race-2020-11-05>
- [22] <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- [23] <https://www.ledger.com/anatomy-of-a-phishing-attack>
- [24] <https://www.bbc.com/news/technology-18419691>
- [25] <https://www.coindesk.com/crypto-criminals-have-already-stolen-1-4b-in-2020-says-ciphertrace>
- [26] <https://arstechnica.com/tech-policy/2011/06/bitcoin->

price-plummets-on-compromised-exchange/

[27] <https://web.archive.org/web/20140210122955/https://www>

[28] <https://blog.coinbase.com/responding-to-firefox-0-days-in-the-wild-d9c85a57f15b>

[29] <https://www.technologyreview.com/2019/08/08/133823/a-attempted-heist-at-coinbase-was-scary-good-even-though-it-failed/>

[30] <https://www.bbc.com/news/world-europe-50821547>

[31] <https://www.theverge.com/2017/7/29/16060344/btce-bitcoin-exchange-takedown-mt-gox-theft-law-enforcement>

[32] <https://bitnodes.io/>

[33]

<https://www.sciencedirect.com/science/article/pii/S0160791X>

[34] <https://www.bbc.com/news/technology-32781244>

[35]

<https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/>

[36] <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/blockchain-full-report.pdf>

[37] The Basics of Bitcoins and Blockchains, Anthony Lewis.

[38] <https://www.investopedia.com/investing/w-centralized-crypto-mining-growing-problem/>

[39]

<https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq4398>

[40] <https://www.coindesk.com/bitcoin-pizza-10-years-laszlo-hanyecz>

[41] <https://www.reuters.com/world/china/what-beijings-new-crackdown-means-crypto-china-2021-05-19/>

[42] <https://www.goldmansachs.com/insights/pages/crypto-a-new-asset-class-f/report.pdf>

[43] <https://www.ft.com/content/c523fa52-25da-4d7e-8378-cc58bd1e6c89>

[44] <https://finance.yahoo.com/news/bitcoin-is-officially-a-new-asset-class-goldman-sachs-103540636.html>

[45] https://advisor.morganstanley.com/scott.altemose/documents/a--altemose/Case%20for%20Cryptocurrency_MAR%2017%202

[46] <https://www.forbes.com/sites/hershshrefin/2021/06/09/bitcoin-bubble-will-pop-when-investors-recognize-bitcoins-huge-negative-impact-on-the-climate/#:~:text=EDT%20%7C4%2C729%20views-,Bitcoin%20Bubble%20Will%20Pop%20When%20Investors>